



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/075,471	02/13/2002	Jeffrey M. Ayars	109905-129462	7533
60380	7590	11/16/2007		
STEVEN C. STEWART REALNETWORKS; INC. 2601 ELLIOTT AVENUE, SUITE 1000 SEATTLE, WA 98121			EXAMINER KLIMACH, PAULA W	
			ART UNIT 2135	PAPER NUMBER
			MAIL DATE 11/16/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/075,471	Applicant(s) AYARS ET AL.	
	Examiner Paula W. Klimach	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 27 August 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-42 is/are pending in the application.
- 4a) Of the above claim(s) 34-42 is/are withdrawn from consideration.
- 5) ☒ Claim(s) 12-17 is/are allowed.
- 6) ☐ Claim(s) 1, 5-6, 8-10, 18-25, 29, 31-33 is/are rejected.
- 7) ☐ Claim(s) 2-4, 7, 11, 24, 26-28 and 30 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

This office action is in response to amendment filed on 08/27/07. The amendment filed on 08/27/07 have been entered and made of record. Therefore, presently pending claims are 1-42.

Response to Arguments

Applicant's arguments filed 8/27/07 have been fully considered but they are not persuasive because of following reasons.

In response to applicant's argument that the examiner's conclusion of obviousness is based upon improper hindsight reasoning, it must be recognized that any judgment on obviousness is in a sense necessarily a reconstruction based upon hindsight reasoning. But so long as it takes into account only knowledge which was within the level of ordinary skill at the time the claimed invention was made, and does not include knowledge gleaned only from the applicant's disclosure, such a reconstruction is proper. See *In re McLaughlin*, 443 F.2d 1392, 170 USPQ 209 (CCPA 1971). None of the information was gleaned from the applicants disclosure since the references, from which the information was derived, are quoted as shown in the rejection below.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge

Art Unit: 2134

generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the arguments to combine references uses both knowledge from the references and knowledge that is generally available to one of ordinary skill in the art

The applicant argued that it is important that an office action rely on objective evidence and specific factual findings with respect to the motivation to combine references. However motivation to combine is found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992).

The applicant argues further that the office action presents no objective evidence of specific factual findings to support its assertion that there was motivation to combine references. However, the office action is only required to meet three criteria to establish a prima facie case of obviousness. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. The rejection below meets all three criteria.

The applicant argues that the relevant portion of the Amino press release is so brief that it can be quoted in its entirety. This is not found persuasive. The portion of the Amino references teaches the information that is quoted and is therefore the reference is adequate.

Art Unit: 2134

The applicant argues that Horstmann does not disclose a tamper resistant digital content recovery module. This is not found persuasive. In the combination of Horstmann and Shear, Shear discloses a Strongbox, that corresponds to the tamper resistant digital content recovery module, since the Strongbox protects the processing environment, column 14 lines 49-60.

Jackson is replaced by the reference Futamura to teach the node of a tree structure. The system then authenticates devices that are downstream.

The newly cited references are shown below to disclose checking the node for compromise.

Election/Restrictions

The applicant maintained claims 1-33 and withdrew 34-42.

The applicant argues that the office action incorrectly characterized claims 1-33 as being classified in 713/194. The applicant argues further that nowhere is reference made to using a physical barrier to protect a cryptographic processing component. This is not persuasive. The claims recite a tamper resistant digital content recovery module, this is broad enough to include a physical barrier.

The election/restriction is therefore correct and final.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person

Art Unit: 2134

having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 5-6, 8-10, 29, and 32-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Horstmann (6,044,469) in view of the article by M2 Presswire ("AMINO COMMUNICATIONS: Amino launches innovative approach to securing broadband communications; New technology provides digital rights protection for streaming content") and further in view of Shear (6, 157, 721) and further in view of the article by Futamura et al (7,149,894 B2).

In reference to claims 1 and 29 Horstmann discloses a software publisher or distributor configurable software security mechanism (title). The apparatus disclosed by Hortmann is a tamper resistant digital content recovery module wherein the tamper resistance is provided by the protection wrapper, which runs code that performs the protection options, selected by the publisher (column 5 lines 2-30). The system of Hortmann discloses a plurality of plain text digital content rendering modules communicately coupled with each other in a hierarchical manner forming a hierarchy of modules (column 5 lines 54-59), with selective combinations of which to be selectively employed to render the recovered digital contents of corresponding types (column 6 lines 10-21), including one of the plain text digital content rendering modules occupying a root position (part 100 Fig. 5) of the hierarchy to exclusively receive the recovered digital contents to be rendered, of all types, from the tamper resistant digital content recovery module (column 6 lines 10-26). The system of Horstman includes one or more storage units to store said tamper resistant module and said plurality of plain text digital content rendering modules (column 6 lines 5-10); and a processor coupled with the one or more storage units to

execute the tamper resistant module and the plurality of plain text digital content rendering modules (column 6 lines 6-22).

Although Horstman discloses recovering protected digital contents, Horstman does not expressly disclose a system to recover protected digital contents of various types in an obfuscated manner.

The article by the M2 Presswire discloses a system that varies the level of encryption in real time depending upon the type and value of content or transaction. Therefore the system recovers protected digital contents in an obfuscated manner and the digital content is of various types (Full Text paragraphs 2-3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to recover protected digital contents of various types in an obfuscated manner as disclosed by the article by M2 Presswire in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because combining proven techniques minimizes the risk to content dynamically without compromising performance.

Although Horstman discloses rendering plain text, Horstmann does not disclose the digital content as defined by the applicant (multimedia digital content).

Shear discloses a system with tamper resistant work factors to protect itself from load modules (abstract). Shear discloses loading modules for computers and set top boxes and therefore the rendering module for multimedia (column 18 lines 45-67). The system of Shear discloses a load module for movies as well as software (column 8 lines 40-56).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the loading module that is tamper resistant as in Shear in the system of Horstmann. One of ordinary skill in the art would have been motivated to do this because defective, bogus and unauthorized computer information can wreak havoc within an electronic system (column 8 lines 14-19).

Although Horstman discloses a content rendering module, Futamura does not disclose root module.

Futamura discloses a hierarchical structure that enables dispersion of a load that is incurred by a public key certificate issuer authority or a registration authority (abstract). The system organizes the data such that there is a tree with a root node and multiple nodes (Fig. 2).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a hierarchical system wherein there is a root and nodes as in Futamura in the system of Hortmann. One of ordinary skill in the art would have been motivated to do this because the tree structure scales up well with size of data and therefore creates an efficient method of organizing data.

In reference to claims 5 and 31, neither Horstmann nor the M2 presswire article disclose a system wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf plain text digital content rendering module, and the non-leaf modules is equipped to verify the immediate downstream module as not having been compromised.

Shear discloses a system wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position

in the hierarchy from the non-leaf plain text digital content rendering module, and the non-leaf modules is equipped to verify the immediate downstream module as not having been compromised (column 6 lines 16-33).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the loading module that is tamper resistant as in Shear in the system of Horstmann. One of ordinary skill in the art would have been motivated to do this because defective, bogus and unauthorized computer information can wreak havoc within an electronic system (column 8 lines 14-19).

Horstmann, M2 presswire and Shear do not disclose the non-leaf module is equipped to verify the immediate downstream module as not having been compromised.

Futamura discloses a hierarchical structure that enables dispersion of a load that is incurred by a public key certificate issuer authority or a registration authority (abstract). The system of Futamura discloses the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf plain text digital content rendering module, and the non-leaf module is equipped to verify the immediate downstream module as not having been compromised (column 7 lines 30-50)

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a hierarchical system wherein there is a root and nodes as in Futamura in the system of Hortmann. One of ordinary skill in the art would have been motivated to do this because it enables the system to disperse the load by sharing the data processing (abstract).

In reference to claim 6, neither Horstmann nor the M2 presswire disclose a system wherein the non-leaf modules is equipped to verify the immediate downstream module not having been compromised at least during initialization.

Shear discloses a system wherein the non-leaf modules is equipped to verify the immediate downstream module not having been compromised at least during initialization (column 6 lines 16-33).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the loading module that is tamper resistant as in Shear in the system of Horstmann. One of ordinary skill in the art would have been motivated to do this because defective, bogus and unauthorized computer information can wreak havoc within an electronic system (column 8 lines 14-19).

Horstmann, M2 presswire and Shear do not disclose the non-leaf module is equipped to verify the immediate downstream module as not having been compromised. Wherein a compromised downstream module is status information.

Futamura discloses a hierarchical structure that enables dispersion of a load that is incurred by a public key certificate issuer authority or a registration authority (abstract). The system of Futamura discloses a system wherein the non-leaf modules is equipped to verify the immediate downstream module as not having been compromised, at least during initialization (column 7 lines 30-50).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a hierarchical system wherein there is a root and nodes as in Futamura in the

Art Unit: 2134

system of Hortmann. One of ordinary skill in the art would have been motivated to do this because it enables the system to disperse the load by sharing the data processing (abstract).

In reference to claim 8, neither Horstmann nor the M2 presswire disclose a system wherein the non-leaf modules is equipped to verify the immediate downstream module as not having been compromised by verifying a signature of the immediate downstream module.

Shear discloses a system wherein the non-leaf modules is equipped to verify the immediate downstream module as not having been compromised by verifying a signature of the immediate downstream module (column 14 lines 49-60).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use the loading module that is tamper resistant as in Shear in the system of Horstmann. One of ordinary skill in the art would have been motivated to do this because defective, bogus and unauthorized computer information can wreak havoc within an electronic system (column 8 lines 14-19).

Futamura discloses a hierarchical structure that enables dispersion of a load that is incurred by a public key certificate issuer authority or a registration authority (abstract). The system of Futamura discloses the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf plain text digital content rendering module, and the non-leaf module is equipped to verify the immediate downstream module as not having been compromised (column 7 lines 30-50). The system checks the certificate that uses a digital signature to prove authenticity.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a hierarchical system wherein there is a root and nodes as in Futamura in the system of Hortmann. One of ordinary skill in the art would have been motivated to do this because it enables the system to disperse the load by sharing the data processing (abstract).

In reference to claims 9 and 32 wherein the digital content of various types comprises streaming media contents of a plurality of media, and of a plurality of format types (column 5 lines 1-7).

In reference to claims 10 and 23 wherein the apparatus is a selected one of a wireless mobile phone, a palm sized personal digital assistant, a notebook computer, a set-top box, a desktop computer, a single processor server, a multi-processor server, and a cluster of coupled systems (column 5 lines 1-7).

In reference to claim 33 wherein the recordable medium is a selected one of a magnetically recordable medium and an optically recordable medium (column 1 lines 9-30)

Claims 18-23 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Horstmann, in view of the article by M2 Presswire, further in view of Shear, and further in view of the article by Futamura et al as applied to claims 1 and 29 above, and further in view of Graunke et al (5, 991, 399).

In reference to claims 18 and 25 Horstmann discloses a software publisher or distributor configurable software security mechanism (title). The apparatus disclosed by Hortmann is a tamper resistant digital content recovery module wherein the tamper resistance is provided by the protection wrapper, which runs code that performs the protection options, selected by the

Art Unit: 2134

publisher (column 5 lines 2-30). The system of Hortmann discloses a plurality of plain text digital content rendering modules communicatively coupled with each other in a hierarchical manner forming a hierarchy of modules (column 5 lines 54-59), with selective combinations of which to be selectively employed to render the recovered digital contents of corresponding types (column 6 lines 10-21), including one of the plain text digital content rendering modules occupying a root position (part 100 Fig. 5) of the hierarchy to exclusively receive the recovered digital contents to be rendered, of all types, from the tamper resistant digital content recovery module (column 6 lines 10-26). The system of Horstman includes one or more storage units to store said tamper resistant module and said plurality of plain text digital content rendering modules (column 6 lines 5-10); and a processor coupled with the one or more storage units to execute the tamper resistant module and the plurality of plain text digital content rendering modules (column 6 lines 6-22).

Although Horstman discloses recovering protected digital contents, Horstman does not expressly disclose a system to recover protected digital contents of various types in an obfuscated manner.

The article by the M2 Presswire discloses a system that varies the level of encryption in real time depending upon the type and value of content or transaction. Therefore the system recovers protected digital contents in an obfuscated manner and the digital content is of various types (Full Text paragraphs 2-3).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to recover protected digital contents of various types in an obfuscated manner as

Art Unit: 2134

disclosed by the article by M2 Presswire in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because combining proven techniques minimizes the risk to content dynamically without compromising performance.

Horstman discloses the tamper resistant digital content recovery module with a root one of the plurality of hierarchically organized plain text digital content rendering module; however Horstman does not disclose verifying the module has not been compromised. Horstman further does not disclose the root verifying an immediate downstream module is uncompromised before transferring the first digital content to the immediate downstream module to further the rendering of the first digital content.

Grauke discloses a method for securely distributing a conditional use private key to a trusted entity on a remote system (abstract). The system of Graunke determines if the system is a trust worthy player (software) before providing the user with the key and therefore access to digital content (column 3 line 53 to column 4 line 7). In the case that the player is compromised the player does not have the ability to perform the cryptographic operation (column 4 lines 7-14).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the check for a trusted (compromised integrity) player and not allow access to digital content based on the verification of the software (module) as in Graunke in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because the integrity of the trusted player is correlated to its ability to perform a cryptographic operation using an asymmetric key pair in a manner that is tamper resistant thereby preventing an unencrypted copy of digital content to be made (abstract).

In reference to claims 19-20 Horstman discloses the tamper resistant digital content recovery module with a root one of the plurality of hierarchically organized plain text digital content rendering module; however Horstman does not disclose verifying the content rendering module.

Grauke discloses a method for securely distributing a conditional use private key to a trusted entity on a remote system (abstract). The system of Graunke determines if the system is a trust worthy player (software) before providing the user with the key and therefore access to digital content (column 3 line 53 to column 4 line 7). The system of Graunke includes a tamper resistant module is equipped to verify the plain text digital content rendering module (Fig. 2). The verification of the module is in response to request from the tamper resistant module (column 4 lines 5-7).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the check for a trusted (compromised integrity) player and not allow access to digital content based on the verification of the software (module) as in Graunke in the system of Horstman. One of ordinary skill in the art would have been motivated to do this because the integrity of the trusted player is correlated to its ability to perform a cryptographic operation using an asymmetric key pair in a manner that is tamper resistant thereby preventing an unencrypted copy of digital content to be made (abstract).

Futamura discloses a hierarchical structure that enables dispersion of a load that is incurred by a public key certificate issuer authority or a registration authority (abstract). The system of Futamura discloses the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the

Art Unit: 2134

hierarchy from the non-leaf module, and the non-leaf module is equipped to verify the immediate downstream module as not having been compromised (column 7 lines 30-50). The system checks the certificate that uses the a digital signature to prove authenticity.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a hierarchical system wherein there is a root and nodes as in Futamura in the system of Hortmann. One of ordinary skill in the art would have been motivated to do this because it enables the system to disperse the load by sharing the data processing (abstract).

In reference to claim 21 wherein the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf module, and the non-leaf module is equipped to verify the immediate downstream module as not having been compromised, by verifying a signature of the immediate downstream modules.

Futamura discloses a hierarchical structure that enables dispersion of a load that is incurred by a public key certificate issuer authority or a registration authority (abstract). The system of Futamura discloses the hierarchy of modules includes a module occupying a non-leaf position in the hierarchy and a module occupying an immediate downstream position in the hierarchy from the non-leaf plain text digital content rendering module, and the non-leaf module is equipped to verify the immediate downstream module as not having been compromised (column 7 lines 30-50). The system checks the certificate that uses a digital signature to prove authenticity.

Art Unit: 2134

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to use a hierarchical system wherein there is a root and nodes as in Futamura in the system of Hortmann. One of ordinary skill in the art would have been motivated to do this because it enables the system to disperse the load by sharing the data processing (abstract).

In reference to claims 23 wherein the apparatus is a selected one of a wireless mobile phone, a palm sized personal digital assistant, a notebook computer, a set-top box, a desktop computer, a single processor server, a multi-processor server, and a cluster of coupled systems (Horstmann column 5 lines 1-7).

In reference to claim 22 wherein the digital content of various types comprises streaming media contents of a plurality of media, and of a plurality of format types (Horstmann column 5 lines 1-7).

Allowable Subject Matter

Claims 12-17 are allowed.

Claims 2-4, 7, 11, 24, 26-28, and 30 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

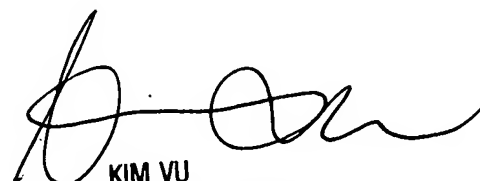
Art Unit: 2134

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PWK

Tuesday, November 13, 2007



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100